Instant Wireless™ Series

Wireless Access Point

Use this guide to install: WAP54A

User Guide

LINKSYS®

COPYRIGHT & TRADEMARKS
Copyright © 2002 Linksys, All Rights Reserved. Instant Wireless™ is a registered trademark of Linksys. Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation. All other trademarks and brand names are the property of their respective proprietors.

LIMITED WARRANTY
Linksys guarantees that every Wireless Access Point is free from physical defects in material and workmanship under normal use for one year from the date of purchase. If the product proves defective during this warranty period, call Linksys Technical Support in order to obtain a Return Authorization Number. BE SURE TO HAVE YOUR PROOF OF PURCHASE AND A BARCODE FROM THE PRODUCT'S PACKAGING ON HAND WHEN CALLING. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. When returning a product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. All customers located outside of the United States of America and Canada shall be held responsible for shipping and handling charges.

IN NO EVENT SHALL LINKSYS' LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS DOES NOT OFFER REFUNDS FOR ANY PRODUCT. Linksys makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Linksys reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to:

Linksys P.O. Box 18558, Irvine, CA 92623.

FCC STATEMENT
This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

UG-WAP54A-040302NC KL

Table of Contents

Chapter 1: Introduction

The Instant Wireless™ Wireless Access Point

Don't be bound by cabling restrictions any longer! The Instant Wireless™ Wireless Access Point from Linksys delivers the freedom to configure your network your way. Utilization of "state-of-the-art" wireless technology gives you the ability to set up workstations in ways you never thought possible; no cables to install means less expense and less hassle.

The Instant Wireless™ Wireless Access Point's high-powered antenna offers a range of operation of up to 328 feet indoors, providing seamless roaming throughout your wireless LAN infrastructure; an advanced user authentication feature ensures a high level of network security. The Instant Wireless™ Wireless Access Point is easy to install (just plug it in and you're ready to go!) and easy to use. With Internet browser-based diagnostics and statistic tools, you're always in control.

When all these features come together in one compact, lightweight, and power-efficient unit, you have the ultimate in flexible networking--the Linksys Instant Wireless™ Wireless Access Point.

Features

- Interoperable with other 802.11a wireless equipment
- Up to 72Mbps turbo mode (only when used with the Linksys WPC54A)
- Up to 64 wireless users (nodes)
- Operation in the uncrowded 5 GHz band
- Enhanced security using up to 152-bit WEP encryption
- MAC address filtering and WEP ensure DSSS security
- Quick and easy setup using your own web browser
- Easy-to-Use Web-Based management
- Free technical support— 24 hours a day, 7 days a week, toll-free U.S. calls
- 1-Year limited warranty

Figure 1-1

Package Contents

- One Wireless Access Point (IEEE 802.11a)
- One Power Adapter
- One User Guide
- Registration Card (not shown)

Minimum Requirements

- One Pentium Class, 200MHz or Faster, PC equipped with Windows 98, Millennium, NT version 4.0, 2000, or XP, 64 MB RAM, and an Ethernet Adapter with Network Cable for Initial Setup
- One 802.11a-compliant Wireless Adapter

Chapter 2: Planning Your Wireless Network

Network Topology

A wireless LAN is a group of computers, each equipped with one Instant Wireless™ Series adapter. Computers in a wireless LAN must be configured to share the same radio channel.

The Instant Wireless™ Series adapters provide access to a wired LAN for wireless workstations. An integrated wireless and wired LAN is called an Infrastructure configuration. A group of Instant Wireless™ Series adapter users and an Instant Wireless™ Wireless Access Point compose a Basic Service Set (BSS). Each Instant Wireless™ Series adapter PC in a BSS can talk to any computer in a wired LAN infrastructure via the Instant Wireless™ Wireless Access Point.

An infrastructure configuration extends the accessibility of an Instant Wireless™ Series adapter PC to a wired LAN, and doubles the effective wireless transmission range for two Instant Wireless™ Series adapter PCs. Since the Wireless Access Point is able to forward data within its BSS, the effective transmission range in an infrastructure LAN is doubled.

Roaming

Infrastructure mode also supports roaming capabilities for mobile users. More than one BSS can be configured as an Extended Service Set (ESS). This continuous network allows users to roam freely within an ESS. All PCs equipped with an Instant Wireless™ Series adapter within one ESS must be configured with the same ESS ID and use the same radio channel.

Before enabling an ESS with roaming capability, choosing a feasible radio channel and optimum Wireless Access Point position is recommended. Proper Wireless Access Point positioning combined with a clear radio signal will greatly enhance performance.

Chapter 3: Getting to Know the Wireless Access Point

The Wireless Access Point's Ports

The Access Point's ports, where a network cable is connected, are located on the Access Point's rear panel, as shown in Figure 3-1.

Figure 3-1

LAN This **LAN** (Local Area Network) port connects to Ethernet network devices, such as a hub, switch, or router.

DC 5V The **Power** port is where you will connect the power adapter.

Reset (Button) Briefly pressing the Reset Button, for approximately ten seconds, will refresh the Access Point's connections, potentially clearing any jammed links.

Important: Resetting the Access Point will erase all of your settings (WEP Encryption, Wireless and LAN settings, etc.) and replace them with the factory defaults. Do not reset the Access Point if you want to retain these settings.

The Wireless Access Point's LEDs

The Access Point's LEDs, where information about the unit's current status is displayed, are located on the Access Point's front panel, as shown in Figure 3-2.

Figure 3-2

Power *Green*. The **Power** LED lights up when the Access Point is powered on.

ACT *Green*. If the LED is flickering, the Access Point is actively sending or receiving data to or from one of the devices on the network.

LINK *Green*. The **LINK** LED serves two purposes. If the LED is continuously lit up, the Access Point is successfully connected to a device through the LAN port. If the LED is flickering, it is an indication of any network activity.

Chapter 4: Connecting the Wireless Access Point

1. **Locate an optimum location for the Access Point.** The best place for the Access Point is usually at the center of your wireless network, with line of sight to all of your mobile stations.

2. **Fix the direction of the antenna.** Try to place it in a position which can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.

3. **Connect a standard Ethernet network cable to the Access Point.** Then, connect the other end of the Ethernet cable to a switch or hub. The Access Point will then be connected to your 10/100 Network.

4. **Connect the AC Power Adapter to the Access Point's Power Socket.** Only use the power adapter supplied with the Access Point. Use of a different adapter may result in product damage.

Now that the hardware installation is complete, proceed to **Chapter 5: Configuring the Wireless Access Point** for directions on how to setup the Access Point.

Note: In order for all other wireless devices to communicate with the Access Point, those devices must be operating in the **Infrastructure Mode**. If any wireless devices are configured in the **Ad Hoc Mode**, they *will not* be recognized by the Access Point.

Chapter 5: Configuring the Wireless Access Point

Important: Before configuring the Access Point, be sure to set up the TCP/IP protocol on your wireless PCs. If this has not already been done, please refer to Appendix B: Setting Up the TCP/IP Protocol.

The Access Point has been designed to be functional right out of the box, with its default settings. However, if you'd like to change these settings, the Access Point can be configured through your web browser with the Web-Based Utility. This chapter explains how to configure the Access Point in this manner.

Open your web browser and enter the Access Point's IP Address, **192.168.1.252**, into the address field. Press the **Enter** key and the following screen, shown in Figure 5-1, will appear. Leave the User Name field blank. The first time you open the Web-Based Utility, use the default password: **admin**. You can set a new password from the Setup tab shown in Figure 5-2. Press the **OK** button to continue or **Cancel** to quit.

Figure 5-1

The Setup Tab

The first tab that appears, shown in Figure 5-2, is the Setup tab. This allows you to change the Access Point's general settings. Change these settings as described here and click the **Apply** button to apply your changes or **Cancel** to cancel your changes. If you require online help, click the **Help** button.

- **Firmware Version.** This displays the current version of the Access Point's firmware. Firmware should only be upgraded if you experience problems with the Access Point and can be upgraded from the Help tab.

- **Access Point Name.** You may assign any name to the Access Point. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network. Verify this is the name you wish to use and click the **Apply** button to set it.

- **LAN:**

  - **IP Address.** This IP address must be unique to your network. We suggest you use the default IP address of 192.168.1.252. As this is a private IP address, there is no need to purchase a separate IP address from your service provider. Verify the address and click the **Apply** button to save changes.

  - **Subnet Mask.** The Access Point's Subnet Mask (or IP Mask) must be the same as your Ethernet network. Verify this is correct and click the **Apply** button to set it.

  - **Gateway.** If a Gateway IP address is required, enter that here.

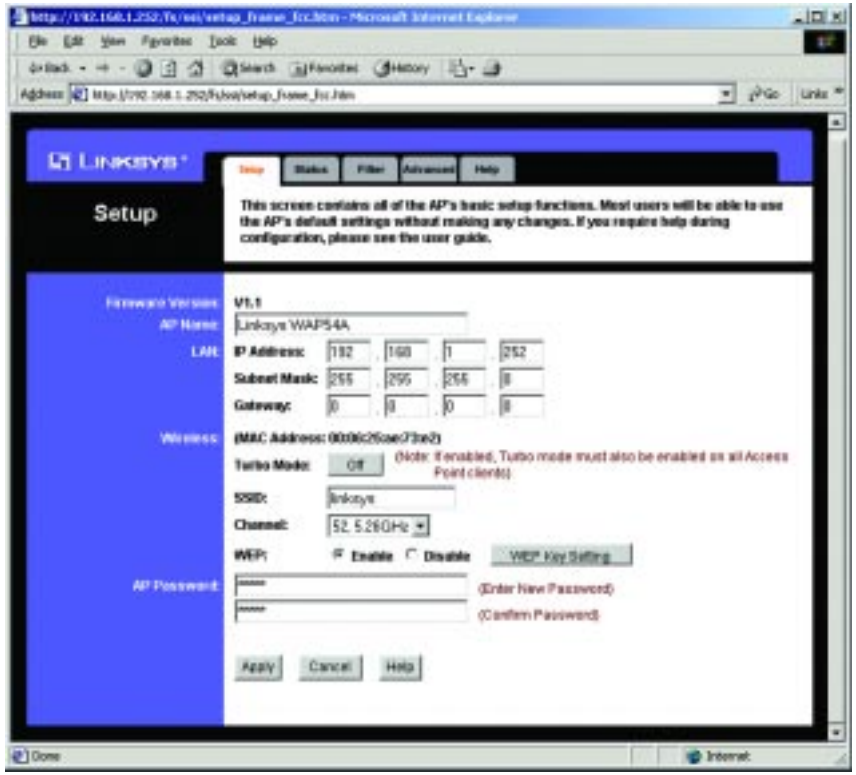

Figure 5-2

- **Wireless:**

  - **Turbo Mode.** Click this button to increase the speed of your wireless transmissions (it will change from **Off** to **On**), keeping in mind that the Access Point's range diminishes in Turbo Mode.

Important: Always remember that, when the Access Point works in Turbo Mode, each point in your wireless network MUST use Turbo Mode as well or your wireless network will not function properly.

  - **SSID.** The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network.

  - **Channel.** Select the appropriate channel from the list provided to correspond with your network settings. All points in your wireless network must use the same channel in order to function correctly.

  - **WEP**. The WEP Encryption method is **Disabled** by default. To enable WEP, click the **WEP Key Setting** button.

Changing the sign-on password for the Access Point is as easy as typing the password into the **AP Password** field. Then, type it again into the second field to confirm.

Click the **Apply** button to apply your changes or **Cancel** to cancel your changes. If you require online help, click the **Help** button.

SETTING WEP ENCRYPTION:

Setting WEP Encryption through the Web-based Browser Utility is done by clicking the **WEP Key Setting** button on the Setup Screen as shown in Figure 5-2.

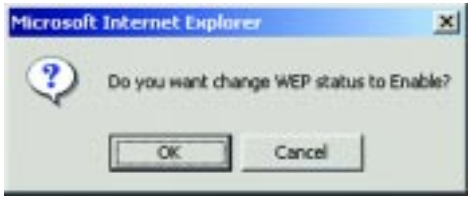

Figure 5-3

A screen will pop up, asking you to confirm the WEP change to mandatory, as shown in Figure 5-3. Click the **OK** button to enable WEP Encryption or **Cancel** to return to the Setup Screen.

Important: Always remember that each point in your wireless network MUST use the same WEP Encryption method and encryption key or your wireless network will not function properly.

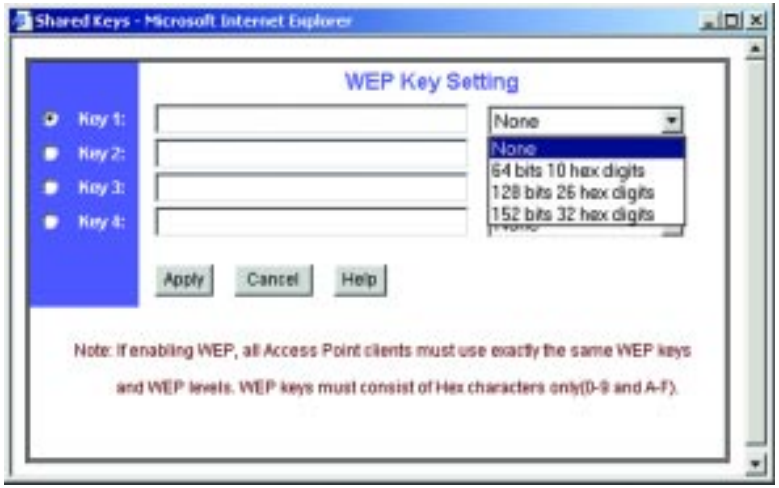

Figure 5-4

This will open the WEP Key Setting screen, Figure 5-4. From this screen, you can select the type of WEP encryption to use.

From the pull-down menu at the top of the screen, select 64-bit, 128-bit, or 152-bit encryption. Then, select the key you wish you use for encrypting your data, Key 1-4. In the field beside the key you've chosen, type the key in Hexadecimal characters, which, on your keyboard, are the letters "A" through "F" and the numbers "0" through "9". Each type of encryption requires a key of a certain length:

64-bit encryption requires a 10 character key.
128-bit encryption requires a 26 character key.
152-bit encryption requires a 32 character key.

Click the **Apply** button to apply your changes or **Cancel** to cancel your changes. If you require online help, click the **Help** button. Clicking the **Apply** or **Cancel** button will return you to the Setup tab. Click either button again on this tab, depending on your choice.

The Status Tab

The "Status" tab, shown in Figure 5-5, will display the Access Point's current MAC address and state as well as the state and MAC Address of each wireless point on your network associated with it.

Figure 5-5

For more information on any device listed, simply click the MAC Address of that device and another screen, shown in Figure 5-6, will appear, displaying details on that device.

Figure 5-6

The Filter Tab

The "Filter" tab, shown in Figure 5-7, allows you to block or allow certain computers, by their MAC Address, from communicating with the Access Point.

To enable filtering of computers by their MAC Addresses, select **Enable** from the drop-down menu. Next, click the **Add** button. This will bring up another screen, as shown in Figure 5-8, where you will specify the MAC Address you will allow or deny over your wireless network.

In MAC Address field at the top of this screen, type the MAC Address(es) you wish to filter. Then, click the Type drop-down menu to select if you will allow access to other MAC Addresses or if you will deny the MAC Addresses.

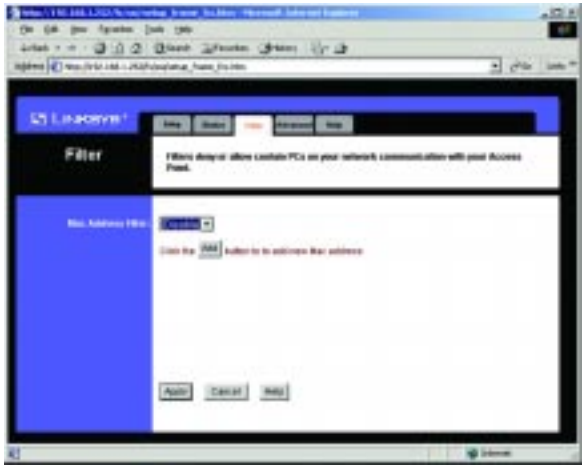

Figure 5-7

To add this to your filtered MAC Addresses, click the **Add to List** button. Click the **Cancel** button to return to the previous screen without saving changes. For more information on this tab, you can click the **Help** button.

When you've completed making any changes on this tab, click the **Apply** button to save those changes or **Cancel** to exit the Web-based Utility without saving changes. For more information on this tab, you can click the **Help** button.

Figure 5-8

The Advanced Tab

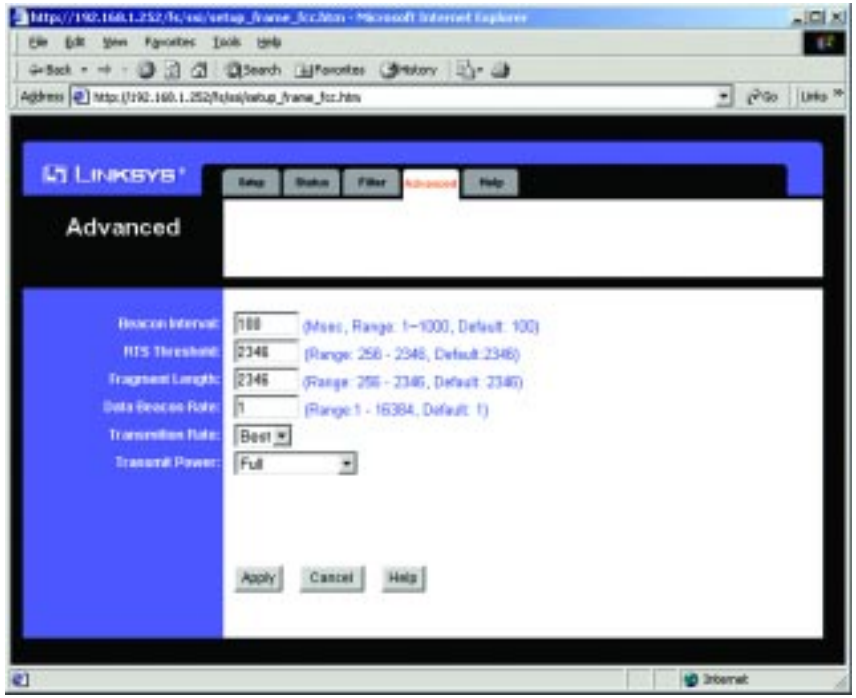

Figure 5-9

Before making any changes to the Advanced tab, shown in Figure 5-9, please check your wireless settings on other systems, as these changes will alter the effectiveness of the Access Point. In most cases, these settings do not need to be changed.

- **Beacon Interval.** This value between 20 and 1000, indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

- **RTS Threshold.** This value should remain at its default setting of 2,346. Setting this parameter to a small value causes packets to be sent more often, consuming more of the available bandwidth and reducing throughput. A higher value, however, sends more packets less often. Should you encounter inconsistent data flow, only minor modifications are recommended.

- **Fragmentation Length.** This specifies the maximum size a data packet will be before splitting and creating a new packet and should remain at its default setting of 2,346. A smaller setting means smaller packets, which will create more packets for each transmission. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

- **Data Beacon Rate.** This value between 1 and 16384, indicates the interval of the Delivery Traffic Indication Message. A Data Beacon Rate field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next message with a rate value. Access Point Clients hear the beacons and awaken to receive the broadcast and multicast messages.

- **Transmission Rate.** The basic transfer rates should be set depending on the speed of your wireless network. Select the most appropriate rate for your network or select **Best**, which will automatically select the optimal transmission rate.

- **Transmission Power.** This option allows you to set the power at which the Access Point transmits. This will allow you to prevent transmission outside your network radius and possible lapses in network security. Selecting a value other than FULL may limit the coverage area and data rates of your wireless PCs.

When you've completed making any changes on this tab, click the **Apply** button to save those changes or **Cancel** to exit the Web-based Utility without saving changes. For more information on this tab, you can click the **Help** button.

The Help Tab

For help on the various tabs in this Web-based Utility, along with upgrading the Access Point's firmware and viewing this User Guide, click the "Help" tab, shown in Figure 5-10.

The help files for the various tabs in this Web-based Utility are listed by tab name on the left hand side of the screen.

Figure 5-10

The following resources require an Internet connection in order to access them.

Click the **Linksys Website** link to connect to the Linksys homepage for Knowledgebase help files and information about other Linksys products.

For an **Online Manual in PDF format**, click that text link. The manual will appear in Adobe pdf format. If you do not have the Adobe PDF Reader installed on your computer, click the **Adobe Website** link to download this software.

Firmware can be upgraded from this tab as well. Do not upgrade your firmware unless you are experiencing problems with the Access Point. To begin the upgrade process, click the Linksys Website link to download the upgraded firmware's ".bin" file from the website. Then, return to this tab and click the **Firmware Upgrade** link.

Upon clicking the Upgrade Firmware link, a new screen, shown in Figure 5-11, will appear requesting the IP Address of the PC upon which the new firmware was downloaded and the location of that firmware ".bin" file. If you do not know the location, click the **Browse** button to locate the file. Then, click the **Upgrade** button to upgrade the firmware, **Cancel** to stop the process, or **Help** for more information about upgrading firmware.

Figure 5-11

Appendix A: Troubleshooting

This chapter provides solutions to problems usually encountered during the installation and operation of the Access Point. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at www.linksys.com.

Frequently Asked Questions

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine if it supports operation over a network.

Can I play multiplayer games with other users of the wireless network?
Yes, as long as the game supports multiple players over a LAN (local area network). Refer to the game's user guide for more information.

What IEEE 802.11a features are supported?
The product supports the following IEEE 802.11a functions:

- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation

What is Ad-hoc?
An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. An Ad-hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

What is Infrastructure?
An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to a central database, or wireless application for mobile workers.

What is Roaming?
Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single Access Point. Before using the roaming function, the workstation must

make sure that it is the same channel number as the Access Point of the dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and Access Point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links Access Points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each Access Point and the distance of each Access Point to the wired backbone. Based on that information, the node next selects the right Access Point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original Access Point or whether it should seek a new one. When a node no longer receives acknowledgment from its original Access Point, it undertakes a new search. Upon finding a new Access Point, it then re-registers, and the communication process continues.

What is BSS ID?
A specific Ad-hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

What is ESSID?
An Infrastructure configuration could also support roaming capability for mobile workers. More than one BSS can be configured as an Extended Service Set (ESS). Users within an ESS could roam freely between BSSs while maintaining a continuous connection to the wireless network stations and Access Points.

What is Spread Spectrum?
Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not

tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?
Frequency Hopping Spread Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct Sequence Spread Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Would the information be intercepted while transmitting on air?
WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, the WLAN series offers the encryption function (WEP) to enhance security and access control. Users can set it up depending upon their needs.

Can Instant Wireless™ products support file and printer sharing?
Instant Wireless™ products perform the same function as LAN products. Therefore, Instant Wireless™ products can work with Netware, Windows NT/2000, or other LAN operating systems to support printer or file sharing.

What is WEP?
WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802.11 standard.

How do I avoid interference?
Using multiple Access Points on the same channel and in close proximity to one another will generate interference. When employing multiple Access Points, be sure to operate each one on a different channel (frequency).

How do I reset the Access Point?
Press the **Reset** button on the back of the Access Point for about ten seconds. This will reset the unit to its default settings.

How do I resolve issues with signal loss?
There is no way to know the exact range of your wireless network without testing. Every obstacle placed between an Access Point and wireless PC will create signal loss. Leaded glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with your Access Point and your wireless PC in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel. Also, due to FCC regulations, more power may be transmitted on channels 52, 56, 60 and 64, than on the lower channels. Lastly, check the Advanced tab of the Web-Based Utility and make sure that FULL is selected in the Transmission Rate field.

Does the Turbo Mode work with Windows XP PCs?
No. The Turbo Mode does not work with Windows XP PCs.

Does the Access Point function as a firewall?
No. The Access Point is only a bridge from wired Ethernet to wireless clients.

I have excellent signal strength, but I cannot see my network.
WEP is probably enabled on the Access Point, but not on your wireless adapter (or vice versa). Verify that the same WEP Keys and levels (64, 128 or 152) are being used on all nodes on your wireless network.

What is the maximum number of users the Access Point facilitates?
No more than 65, but this depends on the volume of data and may be less if many users create a large amount of network traffic.

How many channels are available with the Access Point?
There are eight available channels (frequencies) ranging from 5.15GHz to 5.32GHz.

What is Turbo mode?
Turbo mode allows high-speed connections, but severely limits range. Turbo mode must be enabled on both the Access Point and the wireless PCs to function. Turbo mode is not compatible with Windows XP and may only function with Linksys 5GHz wireless adapters.

What is the difference in range between 802.11a and 802.11b products?
Overall, range will be a little less in a typical environment, while higher speeds may be achieved with 802.11a, throughput degrades more quickly. (See Figure A-1.)

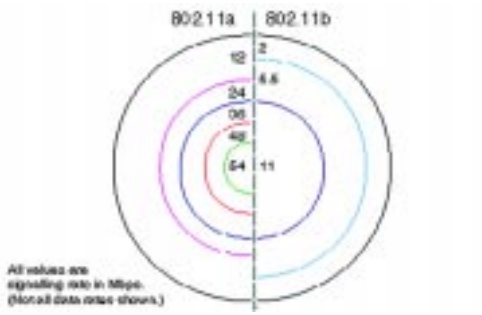

Figure A-1

Are 802.11a and 802.11b products compatible?
No. These products use different frequencies - 5GHz and 2.4GHz respectively.

Will the Access Point be subjected to interference from my microwave or cordless phones?
No. Since the Access Point operates in the uncrowded 5GHz band, there is less interference than ever. The Access Point also has an "Auto Select" feature that scans for clear channels.

Will 802.11a (5GHz) interfere with my 802.11b (2.4GHz) Access Point?
No. Because their signals travel in different frequency bands, one significant benefit is that they will not interfere with each other.

Can I use wireless adapters from other vendors to connect to the Linksys Access Point?
Yes. Any wireless adapter that adheres to the IEEE 802.11a standard should function with the Access Point.

Appendix B: Setting Up the TCP/IP Protocol

Setting Up TCP/IP in Windows

Before a computer can communicate with the Access Point, it must be configured with the TCP/IP protocol. If you know how to set up TCP/IP on your computers, do so now. Otherwise, use the guidelines below to help get TCP/IP installed on all of the computers that need to communicate with the Access Point. If you are unable to successfully install TCP/IP on one or more computers after following the directions, contact the manufacturer of your computers' network operating system for further assistance. Check with your network administrator for your TCP/IP settings.

The directions below provide general guidelines for coming up with IP addresses and subnet masks. Check with your network administrator to see if you need to use specific IP addresses or DHCP settings.

First, each computer on the network will require an IP address, which is a series of numbers, separated by periods, identifying the PC on the network. To make things simple, it is recommended you use the following numbering scheme:

192.168.1.X

In this example, X is a unique, arbitrarily assigned number from 1 to 252. Each computer must have its own unique X number. Note: Never use 0 or 252 for X. These numbers are reserved for other uses.

For example, if you have three computers, you could number them as follows:

192.168.1.17
192.168.1.44
192.168.1.126

In this case, 17, 44, and 126 are arbitrary numbers between 1 and 254.

Each computer will also require a subnet mask, which is a numerical “filter” that tells a computer what kinds of TCP/IP data packets to accept. If you’re not sure which mask to use, the following mask is recommended:

255.255.255.0

The following instructions are provided as examples for reference only. For complete instructions on installing and troubleshooting TCP/IP and IPX, consult your Windows operating system documentation.

TCP/IP Setup for Windows 98 and Millennium

1. Click the **Start** button, select **Settings**, and open the **Control Panel**. Inside the Control Panel, double-click the **Network** icon.

2. If the *TCP/IP Protocol* is listed for your network adapter, go to step five. Otherwise, click the **Add** button.

3. When the **Component Type** window appears, select **Protocol** and click the **Add** button.

4. Select **Microsoft** in the Manufacturers list and choose **TCP/IP** in the Network Protocols list. Then, click the **OK** button.

5. When the Network window reappears, click **TCP/IP** and then click the **Properties** button.

6. Select **Specify an IP Address**.

7. Enter an IP Address for the computer, along with a Subnet Mask. Click the **OK** button. If you do not have these values, consult your network administrator.

8. When the Network window reappears, click the **OK** button. Restart your machine. TCP/IP has now been successfully installed.

TCP/IP Setup for Windows NT 4.0

1. Click the **Start** button, select **Settings**, and open the **Control Panel**. Inside the Control Panel, double-click the **Network** icon.

2. When the **Network** window appears, click the **Protocols** tab. Then, click the **Add** button.

3. Find the **TCP/IP protocol** in the **Select Network Protocol** field. Click on it once and then click the **OK** button.

4. When asked if you want to use DHCP, choose **No**.

5. If asked to supply your Windows NT CD, do so. NT will copy the necessary files to your system. You may have to switch between the Access Point's Setup CD and the NT CD.

6. When TCP/IP appears in the **Network Protocols** window, click the **Bindings** tab. Windows will store your new bindings.

7. Click the **Protocols** tab. Then, select **TCP/IP**.

8. Click the **Properties** button. Select the type of network adapter you have from the Adapters box and select **Specify an IP Address**.

9. Enter the computer's IP Address and Subnet Mask. Check with your network administrator for your settings.

10. Enter your Default Gateway if you have one.

> ***Note:*** *a Default Gateway is not required. Check with your network administrator.*

11. When you finish, click the **OK** button. If NT asks about WINS, ignore it.

12. When the **Network** window reappears, click the **Close** button. Restart your computer when prompted. TCP/IP has now been successfully installed.

TCP/IP Setup for Windows 2000

1. At the Windows 2000 desktop, right click **My Network Places** and select **Properties**. Then, right click **Local Area Connection**. Choose **Properties**.

2. If the *TCP/IP Protocol* is listed for your network adapter, go to step five. Otherwise, click the **Install** button.

3. When the **Component Type** window appears, select **Protocol**, and click the **Add** button.

4. Select **Internet Protocol (TCP/IP)** from the list and click the **OK** button.

5. When the **Local Area Connection Properties** window reappears, select **TCP/IP**, and click the **Properties** button.

6. Select **Use the following IP Address**.

7. Enter an IP Address for the computer, along with a Subnet Mask and Default Gateway. Then, click the **OK** button. If you do not have these values, consult your network administrator.

8. When the **Local Area Connection Properties** window reappears, click the **OK** button. TCP/IP has now been successfully installed.

TCP/IP Setup for Windows XP

1. Click the **Start** button and open the **Control Panel**.

2. Double click the **Network and Internet Connections** icon.

3. Double click the **Network Connections** icon.

4. Right click the **Local Area Connection** icon and select **Properties**.

5. If the TCP/IP Protocol is not installed, click the **Install** button and insert your Windows XP CD. Then, follow the prompts to install TCP/IP.

Appendix C: Glossary

Adapter - Printed circuit board that plugs into a PC to add to capabilities or connectivity to a PC. In a networked environment, a network interface card is the typical adapter that allows the PC or server to connect to the intranet and/or Internet.

Ad-hoc Network - An ad-hoc network is a wireless network or other small network in which some of the network devices are part of the network only for the duration of a communications session while in some close proximity to the rest of the network.

Automatic Rate Selection - Switches the speed when the quality of the link cannot sustain maximum rate. With lower data rates larger distances can be covered. When the user comes closer to the access point, the quality of the link improves and the radio automatically switches back to the maximum.

Backbone - The part of a network that connects most of the systems and networks together and handles the most data.

Bandwidth - The transmission capacity of a given facility, in terms of how much data the facility can
transmit in a fixed amount of time; expressed in bits per second (bps).

Beacon Interval - A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Bit - A binary digit. The value - 0 or 1-used in the binary numbering system. Also, the smallest form of data.

Browser - A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web or PC. The word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files online.

BSS (**B**asic **S**ervice **S**et) - A group of wireless Network PC Card users and an Access Point.

Buffer - A buffer is a shared or assigned memory area used by hardware devices or program processes that operate at different speeds or with different sets of priorities. The buffer allows each device or process to operate without being held up by the other. In order for a buffer to be effective, the size of the buffer and the algorithms for moving data into and out of the buffer need to be considered by the buffer designer. Like a cache, a buffer is a "midpoint holding place" but exists not so much to accelerate the speed of an activity as to support the coordination of separate activities.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - In local area networking, this is the CSMA technique that combines slotted time-division multiplexing with carrier sense multiple access/collision detection (CSMA/CD) to avoid having collisions occur a second time. This works best if the time allocated is short compared to packet length and if the number of situations is small.

CSMA/CD (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **D**etection) - The LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is quiet (senses the carrier). If it is not, it waits a random amount of time before retrying. If the network is quiet and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and each wait a random amount of time before retrying.

CTS (**C**lear **T**o **S**end) - An RS-232 signal sent from the receiving station to the transmitting station that indicates it is ready to accept data.

Database - A database is a collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

Download - To receive a file transmitted over a network. In a communications session, download means receive, upload means transmit.

Driver - A workstation or server software module that provides an interface between a device and the upper-layer protocol software running in the computer; it is designed for a specific device, and is installed during the initial installation of a network-compatible client or server operating system.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) - DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without -the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages.

Dynamic IP Address - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

Encryption - A security method that applies a specific algorithm to data in order to alter the data's appearance and prevent other devices from reading the information.

ESS - More than one BSS in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. Has a transfer rate of 10 Mbps. Forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

FHSS (**F**requency **H**opping **S**pread **S**pectrum) - FHSS continuously changes the center frequency of a conventional carrier several times per second according to a pseudo-random set of channels, while chirp spread spectrum changes the carrier frequency. Because a fixed frequency is not used, illegal monitoring of spread spectrum signals is extremely difficult, if not downright impossible depending on the particular method.

Firmware - Programming that is inserted into programmable read-only memory (programmable read-only memory), thus becoming a permanent part of a computing device.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Hardware - Hardware is the physical aspect of computers, telecommunications, and other information technology devices. The term arose as a way to distinguish the "box" and the electronic circuitry and components of a computer from the program you put in it to make it do things. The program came to be known as the software.

Hub - The device that serves as the central location for attaching wires from workstations. Can be passive, where there is no amplification of the signals; or active, where the hubs are used like repeaters to provide an extension of the cable that connects to a workstation.

IEEE (The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) - The IEEE describes itself as "the world's largest technical professional society, promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members."

The IEEE fosters the development of standards that often become national and international standards. The organization publishes a number of journals, has many local chapters, and several large societies in special areas, such as the IEEE Computer Society.

Infrastructure - An infrastructure network is a wireless network or other small network in which the wireless network devices are made a part of the network through the Access Point which connects them to the rest of the network.

IP Address - In the most widely installed level of the Internet Protocol (Internet Protocol) today, an IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packet across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

ISM band - The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

LAN - A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

MAC (**M**edia **A**ccess **C**ontrol) **Address** - A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; unit of measurement for data transmission.

Multicasting - Sending data to a group of nodes instead of a single destination.

Network - A system that transmits any combination of voice, video and/or data between users.

Node - A network junction or connection point, typically a computer or work station.

OFDM - OFDM (Orthogonal Frequency Division Muliplexing) works by breaking one high-speed data stream into a number of lower-speed data streams, which are then transmitted in parallel. Each lower speed stream is used to modulate a subcarrier. Essentially, this creates a multi-carrier transmission by dividing a wide frequency band or channel into a number of narrower frequency bands or sub-channels.

Packet - A unit of data routed between an origin and a destination in a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

PC Card - A credit-card sized removable module that contains memory, I/O, or a hard disk.

Port - A pathway into and out of the computer or a network device such as a switch or router. For example, the serial and parallel ports on a personal computer are external sockets for plugging in communications lines, modems and printers.

RJ-45 (**R**egistered **J**ack-**45**) - A connector similar to a telephone connector that holds up to eight wires, used for connecting Ethernet devices.

Roaming - The ability to use a wireless device and be able to move from one access point's range to another without losing the connection.

Router - Protocol-dependent device that connects subnetworks together. Routers are useful in breaking down a very large network into smaller subnetworks; they introduce longer delays and typically have much lower throughput rates than bridges.

RTS (**R**equest **T**o **S**end) - An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program." The two major categories of software are "system software" and "application software." System software is made up of control programs such as the operating system and database management system (DBMS). Application software is any program that processes data for the user.

A common misconception is that software is data. It is not. Software tells the hardware how to process the data.

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices.

Spread Spectrum - Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

Static IP Address - A permanent IP address that is assigned to a node in an IP or a TCP/IP network.

Subnet Mask - The method used for splitting IP networks into a series of subgroups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

Switch - 1. A data switch connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A method (protocol) used along with the Internet Protocol (Internet Protocol) to send data in the form of message units between computers over the Internet. While IP takes care of handling the

actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packet) that a message is divided into for efficient routing through the Internet.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

Throughput - The amount of data moved successfully from one place to another in a given time period.

Topology - A network's topology is a logical characterization of how the devices on the network are connected and the distances between them. The most common network devices include hubs, switches, routers, and gateways. Most large networks contain several levels of interconnection, the most important of which include edge connections, backbone connections, and wide-area connections.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network. In a communications session, upload means transmit, download means receive.

UTP - Unshielded twisted pair is the most common kind of copper telephone wiring. Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each signal on twisted pair requires both wires. Since some telephone sets or desktop locations require multiple connections, twisted pair is sometimes installed in two or more pairs, all within a single cable.

WEP (**W**ired **E**quivalent **P**rivacy) - A data privacy mechanism based on a 64-bit, 128-bit, or 152-bit shared key algorithm, as described in the IEEE 802.11a standard.

Appendix D: Specifications

Standards	IEEE 802.11a, 802.3, 802.3u	
Channels	8 Channels (US, Canada)	
Ports/Buttons	One 10/100 Ethernet One Reset Button	
Cabling Type	RJ-45 CAT 5 UTP Cable	
Operating Range	Indoors: Outdoors:	Up to 328 feet (100 m) Up to 1148 feet (350 m)
Data Rate	Up to 72Mbps	
Transmit Power	18dBm	
LEDs	Power, Act, Link	

Environmental

Dimensions	8.9” x 5” x 1.6” (226 mm x 127 mm x 41 mm)
Unit Weight	12 oz. (0.34 kg)
Power	External, 5V DC 2.5A Radio Output: +18dBm (64mW)
Certifications	FCC Class B
Operating Temp.	0ºC to 55ºC (32ºF to 131ºF)
Storage Temp.	0ºC to 70ºC (32ºF to 158ºF)
Operating Humidity	0% to 70% Non-Condensing
Storage Humidity	0% to 95% Non-Condensing

Appendix E: Warranty Information

BE SURE TO HAVE YOUR PROOF OF PURCHASE AND A BARCODE FROM THE PRODUCT’S PACKAGING ON HAND WHEN CALLING. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE.

IN NO EVENT SHALL LINKSYS’S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS DOES NOT OFFER REFUNDS FOR ANY PRODUCT.

LINKSYS OFFERS CROSS SHIPMENTS, A FASTER PROCESS FOR PROCESSING AND RECEIVING YOUR REPLACEMENT. LINKSYS PAYS FOR UPS GROUND ONLY. ALL CUSTOMERS LOCATED OUTSIDE OF THE UNITED STATES OF AMERICA AND CANADA SHALL BE HELD RESPONSIBLE FOR SHIPPING AND HANDLING CHARGES. PLEASE CALL LINKSYS FOR MORE DETAILS.

Appendix F: Contact Information

For help with the installation or operation of this product, contact Linksys Technical Support at one of the phone numbers or Internet addresses below.

Sales Information	800-546-5797 (LINKSYS)
Technical Support	866-242-8558
RMA Issues	949-261-1288
Fax	949-261-8868
Email	support@linksys.com
Web	http://www.linksys.com
FTP Site	ftp.linksys.com

http://www.linksys.com

© Copyright 2002 Linksys, All Rights Reserved.